Plano de combate ao Ransomware

Pedro Couceiro - IPO de Coimbra

4 de Dezembro de 2017

IPO COIMBRA

RANSOMWARE

REPÚBLICA PORTUGUESA
SAÚDE

SNS SERVIÇO NACIONAL DE SAÚDE

IPO COIMBRA

IPO COIMBRA

IPO de Coimbra

- 550 postos de trabalho
- 50 Servidores
- 1000 utilizadores de email
  - 25% dos utilizadores usa correio eletrónico como ferramenta de trabalho
- Ecossistema de aplicações clínicas e administrativas
  - Algumas aplicações legacy, sistemas operativos antigos e tipologias obsoletas em processo de migração.
- Infraestrutura de rede e dados moderna
- Datacenter de última geração

IPO COIMBRA

Ransomware – Primeiro caso

- Médio impacto (menos de 30% dos utilizadores afetados)
- Recuperação imediata dos dados
- Interpretado como acidente isolado
- Medidas tomadas
  - Análise das fraquezas de infraestrutura e dos sistemas afetados
  - Análise e reforço da política de backups
  - Criação de honeypots

- Erro Estratégico: Ignorado o principal fator

IPO COIMBRA

> “the weakest link in a company’s security chain is typically people”

REPÚBLICA PORTUGUESA
SAÚDE

SNS SERVIÇO NACIONAL DE SAÚDE

IPO COIMBRA

IPO COIMBRA

Casos seguintes

- 6 ataques em duas semanas
  - 2 ataques no mesmo dia
- Todos os dados foram recuperados
- Periodos de downtime
- Exemplos:
  - “Clique para ganhar um iphone”
  - “Levante a sua encomenda dos CTT aqui”
  - “Clique para confirmar transferência bancária”

IPO COIMBRA

> RANSOMWARE IS MORE ABOUT MANIPULATING VULNERABILITIES IN HUMAN PSYCHOLOGY THAN THE ADVERSARY'S TECHNOLOGICAL SOPHISTICATION.

REPÚBLICA PORTUGUESA
SAÚDE

SNS SERVIÇO NACIONAL DE SAÚDE

IPO COIMBRA

IPO COIMBRA

Plano de Acção de combate ao Ransomware

- 3 fases

- Fase 1
  - Formação e Sensibilização dos utilizadores

- Fase 2
  - Medidas IT

- Fase 3
  - Investimento em segurança

IPO COIMBRA

Formação e Sensibilização de utilizadores

- Formação dedicada ao tema do Ransomware
  - Obrigatória
- Âmbito geral
  - Profissional, pessoal e familiar
- Boas práticas
- Ética informática
- Comportamento online

IPO COIMBRA

Medidas TIC

- Correção de infraestrutura
- Atualização de sistemas
- Limitação de acesso a dados potencialmente perigosos
  - Pen drives
  - Black Lists públicas de sites de Internet
  - Limitação das permissões especiais de aplicações e utilizadores
- Reforço de regras de firewall
- Reforço de regras de servidor de email
- Backups, backups, backups

IPO COIMBRA


IT'LL COST HOW MUCH TO PROTECT MY COMPANY FROM RANSOMWARE? THAT'S EXTORTION!!!
© D.Fletcher for CloudTweaks.com

IPO COIMBRA

Investimento em segurança

- Atualização de uma plataforma antivírus
- Sistema de backups inteligente centralizado
- Reforço da capacidade de storage para backups
- Sistema de bloqueios de acessos a sites maliciosos em tempo real
- Implementação de uma solução de alarmística

IPO COIMBRA

Objectivo:

REPÚBLICA PORTUGUESA SAÚDE
SNS SERVIÇO NACIONAL DE SAÚDE
IPO COIMBRA

IPO COIMBRA

Conclusões

- Importância da formação
  - Utilizadores e equipas de TIC
  - Ética e boas práticas
- Importância da filtragem de informação
  - Email
  - Internet
- Importância da partilha de recursos entre hospitais
  - Estabelecimento de políticas comuns de gestão de risco, estratégias de combate à fraude, no benchmarking e partilha de informações

IPO COIMBRA

Cibersegurança na Saúde

- Tendência para o aumento do número de ataques
  - Valor da informação
  - Área tradicionalmente menos protegida
- Hospitais nacionais são apanhados em varrimento
  - Ainda não há uma procura por alvos definidos
- Ataques por encomenda
  - Dados específicos

IPO COIMBRA

O futuro

- Trabalho em rede
  - Equipas multidisciplinares a nível do SNS
  - Partilha de informação e recursos
- Plano de cibersegurança
  - Alinhado com a SPMS e normas europeias
  - Incluído nos planos estratégicos
- Desafios
  - RGPD
  - NIS Initiative
  - Novos métodos, procedimentos e funções

IPO COIMBRA

"*True CyberSecurity is preparing for what's next*, not what was last." - Neil Rerup

REPÚBLICA PORTUGUESA
SAÚDE

SNS SERVIÇO NACIONAL DE SAÚDE

IPO COIMBRA